A HIGH-ASSURANCE APPROACH TO CJIS-SP COMPLIANCE WHITE PAPER

SENETAS

Security without compromise

CJIS Data-in-Transit Encryption Standards

How to address your Criminal Justice Information Services Security Policy (CJIS-SP) obligations

For US law enforcement agencies, complying with the Criminal Justice Information Services Security Policy (CJIS-SP) has become an imperative. However, it is also essential that any security systems in place do not impede staff from fulling their primary duty – fighting crime.

In this paper, we examine the role of encrypting data in motion – a core component of CJIS-SP compliance. We also offer insights into how organisations can address their data in motion obligations without impacting on network or application performance.

RISK VERSUS RELIANCE

Like most industry sectors, law enforcement has undergone a sustained period of "digital transformation". The rise in mobility, ubiquitous connectivity, big data sharing and the Internet of Things have forever changed the way law enforcement agencies, gather, analyse and exchange information.

Like many organisations, law enforcement has become dependent upon high-speed networking solutions to carry on business as usual. Improvements in connection speed, bandwidth and resilience have transformed the way organisations collaborate and share data; both inter-departmental and intra-agency.

Nobody can argue the advantages gained from greater collaboration and instant access to accurate information – especially in terms of an agency's ability to catch the bad guys. However, the very nature of the networks we have come to rely upon presents a new type of risk.

The high-speed private and public network infrastructure that transports sensitive data to and from CJIS repositories is vulnerable to cyber-attack. The sensitive, and potentially valuable, nature of the data transmitted across the CJIS network means it is a high-profile target for criminals or rogue nation states.

Cyber criminals have become increasingly sophisticated and effective at evading network defences; resulting in the proliferation of high-profile hacks or data breaches that have dominated the headlines over the past 5 years.

Government and defence agencies are just as vulnerable as commercial organisations.

In 2016, over 20% of incidents involved local or central government agencies. Whilst high profile breaches, such as the Clinton campaign or the US Department of Personnel Management, are grabbing the headlines, the impact of data breaches is being felt throughout the law enforcement community.

Across the world, everyone from the US State Department and the Australian Federal Police Department to the Californian DMV, Thames Valley Police in the UK and Anoka County Sheriff's Office are suffering breaches.

This approach enables organisations to select the solution that best suits their specific objectives and core infrastructure; ensuring long-term improvements in security, performance and agility.

CJIS SECURITY POLICY

Given the sensitive, highly critical nature of the information that is exchanged within and among law enforcement agencies, standards have been developed to ensure rigorous safeguards are put in place.

The CJIS-SP was instituted to provide an extensive set of guidelines and requirements surrounding the security of the source, transmission, storage and generation of criminal justice information (CJI).

The CJIS-SP applies to any organisation that has access to CJI at any point in its lifecycle, from creation through dissemination. Organisations responsible for meeting these standards are also subject to regular compliance audits from the FBI's CJIS division.

The core objective of the CJIS Security Policy is to "provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit." When it comes to data in transit, the policy states: "When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption)."

NB: A full copy of the policy is available to download from the FBI website: **https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center**

The definition of when encryption is required is worth clarifying. "Outside the boundary of the physically secure location" includes data transmitted between secure office locations within the same agency.

In recent audits, security teams have been made aware that encryption is required for the transmission of data between a single agency's distributed offices, just as it is when data is shared between different agencies.

The CJIS-SP offers both strategic and tactical guidelines, enabling regulated agencies to select the security mechanisms that are aligned with their specific requirements. The policy defines a set of standards and requirements. Whilst compliance is obligatory, it is important to stress that compliance itself is secondary to ensuring the security of CJI.

To this end, security teams should look to employ technologies and solutions that strengthen the organisation's controls around information access, sharing and storage. The objective should be to determine the most effective security policy and to invest in the best security solutions available; providing the best possible protection against evolving cyber-threats.

A further, but no less important consideration, is to ensure that any security mechanisms put in place do not inhibit users' ability to effectively carry out their day to day tasks. In short, security should not come at the expense of performance.

Encrypting data in motion

In this section, we review some of the alternative approaches to encryption that meet the CJIS-SP compliance standard. We also outline some key characteristics to consider when evaluating your options.

Most of today's networks are IP-based. This presents IT security teams with two fundamental decisions to make: how are they going to encrypt the data and at what layer of the OSI model?

In most cases, the choice comes down to:

> Layer 2 Data Link encryption or Layer 3 IPSec encryption

> Dedicated appliance versus integrated device

LAYER 2 VERSUS LAYER 3

In terms of security and network performance. Layer 2 encryption offers several advantages over Layer 3.

Layer 2 encryption provides better bandwidth utilisation and significantly lower latency. At Layer 2, full line-rate performance can be achieved; maximising the efficiency of your network and protecting your investment in bandwidth.

By comparison, encrypting at Layer 3 can result in the loss of up to 70% of available bandwidth, as the encryption adds a significant network overhead. This bandwidth penalty only increases as the network scales to include more connections and increased bandwidth per connection.

When it comes to latency, the story is similar. At Layer 2, latency is typically measured in microseconds. At Layer 3, it is often measured in milliseconds. This ten-fold increase in latency makes Layer 3 IPSec encryption unsuitable for latency-sensitive applications such as real-time video streaming or financial transactions.

Further, Layer 2 solutions provide consistent latency performance for all packet sizes. Layer 3 solutions often have variable latency, depending on packet size, causing what is known as "jitter"; which can wreak havoc on real-time applications.

In summary, whilst implementing an encryption solution at Layer 3 is typically a lower-cost alterative at the outset, the negative impact on network performance, scalability and reliability result in a higher long-term TCO.

Layer 2 encryption solution may require a higher initial capital outlay, but the security, network and application performance benefits result in an improved ROI and TCO over the lifetime of your investment.

DEDICATED VERSUS INTEGRATED

When it comes to the choice between dedicated encryption hardware and network devices with encryption "built-in", IT security professionals are typically weighing up a price versus risk equation.

As the name would suggest, a dedicated device is built from the ground up with one task in mind. They are designed to be network and vendor-agnostic, providing support for all topologies and use cases.

Integrated, or hybrid, devices are typically routers, switches or other network devices with an element of security built-in. They are multi-function devices, offering a host of services on a single platform.

To maximise security and performance, it is recommended that network and security architectures are kept separate.

Encryption and network routing represent two very different functions, and running one platform that does two dissimilar things can mean that neither is done very well. From a security standpoint, integrated solutions often allow numerous users virtual and physical access.

This increases the probability that the data or keys may be compromised; it also affects performance. As the processing requirement increases, the encryption component of the solution can become sluggish, forming a bottleneck.

Another concern is "vendor lock-in" as in-line security solutions are not compatible with other vendors' solutions. As a result, all future networking and security equipment will be tied to a single vendor, or a "fork-lift upgrade" will be required to replace.

In summary, decoupling security from switching and leveraging Layer 2 Ethernet platforms has become best practice for many agencies. This approach enables organisations to select the solution that best suits their specific objectives and core infrastructure; ensuring long-term improvements in security, performance and agility.

What to look for in a Layer 2 encryption solution

Compliance with the CJIS-SP standards is just the beginning for many agencies. Beyond ticking the box on encryption, security-conscious organisations are looking to employ best-of-breed solutions.

Only by implementing a truly robust encryption solution can they be sure that their data remains protected, even in the event of a breach.

MULTI-CERTIFIED

The CJIS-SP states that "When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards." Look for appliances that are certified FIPS 140-2 Level 3, as well as certification by other independent testing authorities, such as Common Criteria or NATO.

HIGH-ASSURANCE

Not all encryption solutions are created equal. To offer high-assurance protection, an encryption solution needs to meet four key criteria. It should feature:

> Secure, tamper-proof devices; dedicated to network data encryption

> State-of -the-art, automatic, zero-touch cryptographic key management

> End-to-end, authenticated encryption

> Standards-based encryption algorithms

CRYPTO-AGILE

To provide long-term data protection in a post-quantum computing world, encryption solutions need to offer unprecedented levels of versatility. Crypto-agility is about more than simple performance statistics; it comes from compatibility and interoperability, from FPGA-based flexibility and from the ability to support custom cryptographic elements. It even enables a choice of encryption algorithms and standards.

The CJIS-SP mandates a minimum 128-bit encryption. To ensure longer-term data protection, look for a solution that supports 256-bit encryption algorithms that meet recognised standards, such as RSA or ECC.

KEY MANAGEMENT

Look for platforms that provide uncompromising protection of cryptographic keys. These keys should always be kept in a certified (tamper-proof) hardware appliance. There is no reason why your encryption keys should be made available to anyone else; look for a solution that keeps your keys "client-side".

TRUE RANDOMNESS

The strength of your encryption solution is determined by the nature of the random numbers generated to seed your encryption keys. The greater the degree or randomness (entropy), the more secure the key.

Solutions with a hardware source of entropy offer more security than those that rely upon software-generated numbers. The latter can become derivative over time and take time to "cycle-up" when first switched on. For the ultimate in key security, look for a platform that supports quantum key distribution (QKD).

METADATA PROTECTION

The CJIS-SP standard mandates the need to protect meta data from the cloud provider, indicating "The metadata derived from CJI shall not be used by any cloud service provider for any purposes."

The metadata associated with network traffic can ultimately provide intelligence that can expose your organisation. Look for offerings that can protect network metadata by combining traffic flow security (TFS) with Layer 2 Ethernet encryption; making traffic patterns and characteristics impervious to exposure through nefarious traffic analysis.

This is especially critical for organisations that choose to work with cloud providers. Moreover, this will protect your metadata from being exposed by third parties or anyone else who is trying to hack your data and metadata.

PERFORMANCE & AVAILABILITY

For the users in your organisation, gaining timely, dependable access to CJI is critical. Delays can compromise a range of efforts, including emergency response and cross-agency collaboration. Encryption should not have a negative impact on network or application performance and availability. Look for a platform that offers:

High throughput. Appliances should provide the performance required to secure time-sensitive communications and applications. Look for appliances that can run in full duplex mode, at full line speed, without introducing packet loss.

Low latency. Encryption should introduce minimal, consistent latency that is not affected by packet size. Make sure your solution also minimises jitter, which can adversely affect the user experience, particularly for voice over IP (VoIP) and video applications.

PREDICTABILITY

Look for hardware-based "cut through" architecture that supports field-programmable gate array (FPGA) capabilities and delivers predictable, dependable performance.

Reliability is just as important for the IT team as it is for the end-user. Look for platforms that have been proven to run for years, without incident, in performance-intensive environments.

Platforms should provide at least 99.95% uptime. Also look for adherence to industry safety and environmental standards.

FLEXIBILITY

The encryption requirements of your organisation will often vary substantially from those of another. Further, the requirements and priorities your platform needs to address may change over time. Adopt a pragmatic, long-term view of your solution and how it might adapt to address your evolving needs over time.

Look for solutions that are compatible with leading network protocols such as Ethernet, STP (Spanning Tree Protocol) and Shortest Path Bridging (SPB).

These solutions should also offer support for deployment in Ethernet networks with various architectures; ranging from point-to-point to fully meshed. They should also support unicast, broadcast, and multi-cast environments.

Finally, they should be optimised for LAN/MAN/WAN environments; enabling full-path encryption, rather than hop-to-hop encryption.

SCALABLE THROUGHPUT

Look for platforms that can meet your organisation's throughput demands, both initially and in the long term. There are solutions available that offer rate-limited options to meet modest bandwidth requirements of 10-100Mbps, with the ability to scale up to 10Gbps over time.

DEPLOYMENT OPTIONS

Any Layer 2 encryption solution you select should offer support for both single-site deployments and complex environments with multiple locations. Look for vendors that offer a range of products that support the same protocol. Interoperability and backwards compatibility are key to providing a long-term return on your investment.

EASE OF MANAGEMENT

If you need to manage multiple appliances, look for a platform that offers an intuitive web-based management interface. One that enables centralised deployment of encryptors with "set and forget" simplicity.

EASE OF IMPLEMENTATION

Look for a "bump-in-the-wire" solution that allows you to install a device on the network without having to change the architecture and without impacting on the performance of other network devices. Also look for link-state forwarding that supports transparent implementation.

CONCLUSION

Addressing CJIS-SP requirements for data-in-transit encryption represents a baseline requirement for many law enforcement agencies today. However, security teams should focus their efforts on more than compliance and take the steps necessary to maximise the security of the sensitive data they work with.

While the standard offers a lot of clear guidance, the reality is that organisations should select the best solution to secure their data and meet CJIS-SP requirements. By leveraging the right Layer 2 encryption platform, agencies can ensure not only that they'll pass their upcoming CJIS audits and optimise their high-speed network utilisation, but most importantly, they'll strengthen their ability to guard against cyber-threats.

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN Series High-Assurance Encryptors and CV Series Virtual Encryptors are distributed and supported by Gemalto, the world's largest data security company, as SafeNet Ethernet Encryptors.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, data network providers, Cloud and data centre service providers, telecommunications companies and network security specialists.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' own data network service providers, systems integrators and information security specialists to specify the optimal encryption solution for their needs.

Wherever you are, simply contact Senetas or Gemalto directly to discuss your needs. Or, if you prefer, your service provider may contact us on your behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your Layer 2 Ethernet network security needs, Senetas has an encryption solution to suit. They support data network links from modest 10Mbps and 100Mbps bandwidths to high speed 1Gbps, 10Gbps and even ultra-fast 100Gbps networks.

SENETAS CORPORATION LIMITED

E info@senetas.com

www.senetas.com

Senetas designs, develops and deploys high-assurance network data encryption solutions. Designed for today's core Metro Area and Carrier Ethernet WAN infrastructures, Senetas solutions support all Layer 2 protocols and topologies.

Our multi-certified CN Series hardware encryptors have crypto-agility built in and are used by some of the world's most secure organisations; including governments and defence forces, commercial and industrial enterprises, Cloud, data centre and telecommunications service providers in more than 35 countries.

gemalto

www.gemalto.com

Senetas CN Series certified high-assurance network encryptors and CV Series virtual encryptors are distributed and supported internationally by Gemalto (North America, Europe, Asia, Middle East and Africa) as SafeNet Ethernet Encryptors.

CJISSP-WP0917